IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	CRIMINAL NO. 03-
	)	
v.	)	Count 1: Conspiracy
	)	(18 U.S.C. § 371)
HEW RAYMOND GRIFFITHS,	)	
a/k/a "bandido,"	)	Count 2: Criminal Infringement of a
	)	Copyright
Defendant.	)	(17 U.S.C. § 506(a)(1) and 18 U.S.C. § 2319 (b)(1) and (2)

INDICTMENT

MARCH 2003 TERM at Alexandria, Virginia

Count One

THE GRAND JURY CHARGES THAT:

1. Beginning no later than January 1999, and continuing until on or about December 11, 2001, in the Eastern District of Virginia and elsewhere, the defendant, HEW RAYMOND GRIFFITHS, also known by his screen nickname "bandido," conspired and agreed to willfully infringe copyrights with others known and unknown to the grand jury, including but not limited to John Sankus (a.k.a. "eriFlleH"), Christopher Tresco (a.k.a. "BigRar"), David Grimes (a.k.a. "Chevelle"), Richard Berry (a.k.a. "Flood"), Roy Kartadinata (a.k.a. "Tenkuken"), and an individual known by the screen nickname "EvilTea;" that is, during a 180-day period, defendant did conspire and agree to reproduce and distribute at least ten infringing copies of one or more copyrighted works, with a total retail value of more than $2,500, for purposes of private financial gain, in violation of 17 U.S.C. § 506(a)(1), and 18 U.S.C. § 2319(b)(1).

2. It was part of the conspiracy that the defendant and others, including the five coconspirators identified by name in Paragraph 1 above, were members of an Internet software piracy group known as Drink Or Die (DOD). DOD was a highly structured criminal organization devoted to the unauthorized reproduction and distribution of copyrighted software over the Internet. The group sought to achieve a reputation as the fastest provider of the highest quality application and utility software (e.g., Symantec security software, Microsoft and AutoDesk applications) to the underground Internet software piracy community known as the "warez scene."

3. It was further part of the conspiracy that DOD achieved its reputation as a leading provider of new software to the warez scene through a multi-staged process referred to as the group's "release work." DOD's release work was coordinated through a "drop site," a secure computer site hosted by group member Christopher Tresco (a.k.a. "BigRar") on the computer network of the Massachusetts Institute of Technology in Boston, Massachusetts. Access to the drop site was strictly controlled by defendant GRIFFITHS and a few other high-level group members through a combination of security measures that included password protection and user and IP address verification. DOD members known as "suppliers" would upload new software to the group's drop site sometimes days or weeks before the manufacturer's public release date. Once new supply was posted to the drop site, other group members known as "crackers" would remove the software from the drop site and apply their special programming skills to "crack" the software's embedded copyright protections. Once cracked and re-posted to the drop site, other DOD members known as "testers" would quality test the software to ensure that the "crack" worked and that the software remained fully functional, then "packers" would break apart the

software into smaller data files that could be more easily distributed over the Internet. Finally, group members known as "pre-ers" (or couriers) prepared the final warez product for release and distribution to at least eight group-affiliated FTP sites throughout the world. FTP sites are computer storage sites running File Transfer Protocol, the communication protocol preferred by most warez groups for transferring files between computers connected to the Internet. Every "cracked" software title released by DOD would include a ".nfo" file that attributed credit for the release to DOD.

4. It was further part of the conspiracy that whenever newly "cracked" software was released by the group, a member of DOD's senior leadership, including defendant GRIFFITHS, would send an e-mail to other DOD staff members announcing the release and attributing credit to individual group members (by screen nickname only) for the supply, crack, pack, test, and pre-ing of the release. In addition to these e-mails, which were referred to within the group as "chili mails," DOD also chronicled their release work by maintaining monthly summary reports of all releases on the drop site at MIT. For instance, the "chili mails" and monthly release reports from November 2000 through December 11, 2001, indicated that DOD cracked and released more than 275 application and utility software programs worth more than $1,000,000. DOD's "pre-ers" (or couriers) would upload each new "release" to a minimum of eight (8) FTP sites worldwide within minutes of its initial distribution from the group's drop site at MIT.

5. It was further part of the conspiracy that DOD was a highly structured, hierarchical organization in which rank and position were determined by a variety of factors, including special skills, length and quality of service to the group, and reputation within the warez scene generally. DOD generally had either one Leader or two co-Leaders, 2-3 Council, 12-15 Staff, and a general

membership comprising approximately 40 individuals. The Leaders had ultimate authority over all aspects of the group; Council members assumed primary responsibility for the group's day-to-day operations, including the group's "release work" and security issues; Staff were generally the most active in the group's day-to-day release work, or in maintaining the group's FTP sites; and general members contributed to the group in a variety of ways, including acting as occasional suppliers of new software, hosting the group's FTP sites, or providing hardware (e.g., laptops, hard drives, routers, and other computer equipment) to other group members for use in their illegal warez activities. The defendant was a longtime Council member in DOD before being officially promoted to co-Leader with an individual using the screen nickname "EvilTea" (a.k.a. "The Evil Adviser") in early 2001. Both as Council and co-Leader, defendant GRIFFITHS exercised control over virtually every aspect of the group's "release work" and its affiliated FTP sites, including: the recruitment of new members; the removal of non-producing members from the group; the promotion of existing members to new leadership positions; adding and deleting users from the group's FTP sites; and leading group business meetings online. On or about July 2001, EvilTea stepped down from his leadership post, and defendant GRIFFITHS promoted then-Council member John Sankus (a.k.a., "eriFlleH")to replace EvilTea as co-Leader.

6. It was further part of the conspiracy that DOD staff members would communicate about the group's illegal activities with other group members through closed, invite-only Internet Relay Chat (IRC) channels, including the channels "#drinkordie," "#dod," and "#fatalerror." Group business and coordination was also conducted via the group's private e-mail server, which was hosted and operated by DOD member Roy Kartadinata (a.k.a. "Tenkuken"). The e-mail server provided individual DOD members with personal e-mail accounts (e.g.,

bandido@drinkordie.com). Defendant GRIFFITHS exercised administrative authority over the member and group list accounts on the e-mail server. The server also provided group e-mail accounts – such as accounts for "DODcrack," DODstaff," and DODsupply" – in order to facilitate communication by DOD leadership, including defendant GRIFFITHS, with group members who performed like functions in DOD. Many e-mails that concerned the group's piracy activities, including the so-called "chili mails" announcing each of the group's new releases, were encrypted as an added security precaution to avoid detection by law enforcement.

7. It was further part of the conspiracy that, to reward and motivate its members, DOD maintained a number of FTP "leech" sites containing tens of thousands of copies of copyrighted software, games, movies, and music that were available for copying and downloading (i.e., "leeching") by group members and other supporters of DOD's illegal activities. Access to these FTP sites was strictly controlled by DOD's highest leadership, including defendant GRIFFITHS. For instance, defendant GRIFFITHS had "site op" authority -- that is, the power to add or remove authorized users -- on all the group's FTP sites, including the sites known as Fatal Error (games and movies), Packet Storm (application and utility software), Lake of Fire (music), and High Octane (software, games, movies, music videos). High Octane was hosted by DOD member David Grimes (a.k.a. "Chevelle") in Arlington, Texas; Packet Storm and Lake of Fire were hosted on the MIT computer network in Boston, Massachusetts, by DOD Staff member Chris Tresco (a.k.a., "BigRar"); and Fatal Error was hosted from March through October, 2001, in the Eastern District of Virginia.

8. It was further part of the conspiracy that DOD's FTP sites were protected by a variety of sophisticated security mechanisms to insure that only authorized users could gain access to the

tens of thousands of software, game, movie, and music titles stored on the sites. Among other security precautions, the sites could only be accessed through known "bounce boxes" by users with pre-approved passwords and IP addresses. As used here, "bounce box" refers to a computer connected full-time to the Internet that automatically re-routes users to another computer on the Internet (the actual FTP site) assigned a different IP address. As a leader in DOD, defendant GRIFFITHS oversaw the maintenance and operation of all the group's FTP sites, including issues involving site access and security.

9. It was further part of the conspiracy that on September 9, 2001, defendant GRIFFITHS participated in an international telephone conference with DOD leadership and staff, including DOD co-Leader John Sankus (a.k.a. "EriFlleH"), and staff members Richard Berry (a.k.a. "Flood"), and Christopher Tresco (a.k.a. "BigRar"). Defendant GRIFFITHS led the discussion of numerous topics concerning the group's piracy activities, including: the need for DOD staff to make greater use of PGP encryption when sending e-mails about group business; ensuring site access to DOD-affiliated FTP sites for DOD staff; the need to recruit more "top quality suppliers" and "one or two more crackers;" and ways to find additional sources of new supply (software) in order to increase the number of cracked software titles released by DOD.

Overt Acts

It was further part of the conspiracy that one or more of the following acts in furtherance of and to effect the objects of the above-described conspiracy were committed in the Eastern District of Virginia:

1. On February 3, 2001, defendant Hew Raymond GRIFFITHS (a.k.a. "Bandido") corresponded via IRC with another group member known as "bcre8tiv," who was

then residing in the Eastern District of Virginia. In that IRC chat session, GRIFFITHS discussed "bcre8tiv" sending him computer parts so that GRIFFITHS could reward other contributing members of DOD such as "Forcekill" (cracker) and "Azide" (supplier). In that same IRC conversation, GRIFFITHS asked "bcre8tiv" whether he had been successful in finding a new "line" (Internet connection) for the DOD "leech" site known as Fatal Error (FE). "Bcre8tiv" responded that "eri" (short for "eriFlleH," the screen name of John Sankus) would be "traveling down weekend after next" to install Fatal Error on a new line.

2. On February 20, 2001, in the Eastern District of Virginia, at defendant GRIFFITHS' request, "bcre8tiv" shipped computer parts via Federal Express package service (FedEx Tracking # 8259 3078 7287) to "Hew Griffiths, 11-30 Lorraine, Bateau Bay, NSW, Australia 2261." On February 26, 2001, at 10:27 am, defendant GRIFFITHS accepted delivery of the package at 11/30-32 Lorraine Street, Berkley Vale (Bateau Bay), Australia.

3. On March 3, 2001, DOD leader John Sankus (a.k.a. "eriFlleH") drove from Philadelphia, Pennsylvania, to Fairfax, Virginia, for the sole purpose of delivering and connecting to the Internet three computer units which, collectively, comprised the DOD "leech" site known as Fatal Error. At the time, Fatal Error contained approximately 550 gigabytes of pirated computer software, games, and movies, of which more than 100 titles had been provided (uploaded) by defendant GRIFFITHS in December 2000 and January 2001. On March 3, 2001, coconspirator John SANKUS (a.k.a. "EriFlleH") assisted in installing Fatal Error at the computer facilities of an Internet Service Provider (ISP) located in Dulles, Virginia.

4. Fatal Error continued to operate at that ISP in Dulles, Virginia, for the benefit of DOD members and others engaged in illegal Internet software piracy, until on or about

October 25, 2001, when Fatal Error was shipped to DOD Staff member Chris Tresco in Boston, Massachusetts. During that same period of time, the "bounce box" used to access Fatal Error was also located in the Eastern District of Virginia, hosted by DOD Staff member Richard Berry (a.k.a. "Flood") on the computer system of Berry's employer in Alexandria, Virginia. While Fatal Error was located in Dulles, Virginia, defendant GRIFFITHS exercised his "site op" authority to grant access privileges, for uploading and downloading, to numerous new users, including, but not limited to, users identified by the screen nicknames "cyclops" (added March 8, 2001), "grogg" (added March 8, 2001), "arma" (added March 13, 2001), "PsedO" (added March 15, 2001), "hando" (added March 16, 2001), "ParisAngel" (added March 27, 2001), and "mrpumpkin" (added June 28, 2001). By November 2001, Fatal Error had grown to contain approximately one (1) Terabyte (more than 15,000 titles) of pirated software, games, and movies. 5. During the eight months in which it was located in the Eastern District of Virginia, more than 9,000 individual titles of pirated software, games, and movies were uploaded to Fatal Error, and more than 18,000 copies of pirated software, games, and movies were downloaded from the site, by DOD members and others engaged in Internet software piracy. During that same time period, GRIFFITHS personally uploaded approximately 32 pirated games to the site.

(All in violation of Title 18, United States Code, Section 371.)

Count Two

THE GRAND JURY FURTHER CHARGES THAT:

1. Between December 1, 2000, and December 11, 2001, in the Eastern District of Virginia and elsewhere, the defendant, HEW RAYMOND GRIFFITHS, also known as "bandido," did willfully, and for the purpose of private financial gain, infringe the copyrights of copyrighted works, to wit, copyrighted software, computer games and movies, by the reproduction and distribution over the Internet, during a 180-day period, often (10) or more copies of one or more of the copyrighted works having a total retail value of $2,500 or more.

(All in violation of Title 17 U.S.C. §506(a)(1) and 18 U.S.C. §2319 (b)(1) and 2.)

A TRUE BILL

_____

F O R E P E R S O N
UNITED STATES GRAND JURY

_____

Paul J. McNulty
United States Attorney

_____

Justin W. Williams
Assistant United States Attorney
Chief, Criminal Division

_____

Robert W. Wiechering
Assistant United States Attorney
Eastern District of Virginia

_____

Michael DuBose
Senior Counsel, Computer Crime & Intellectual
Property Section
Department of Justice